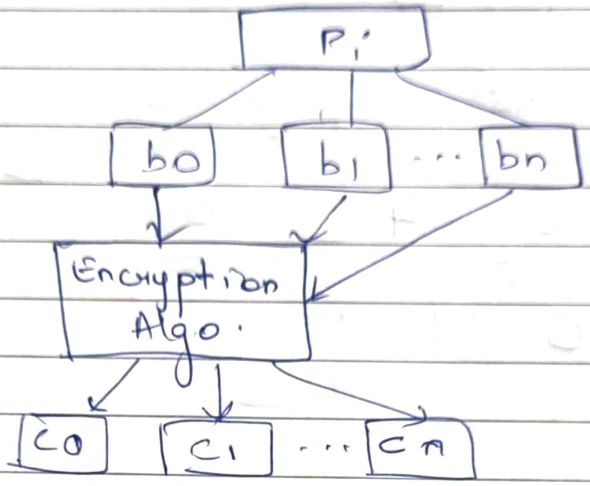
__/__/____

Decryption:

(4-4) (6-5) (5-3) (5-2)

= 0 1 2 3

- Block cipher Tech.

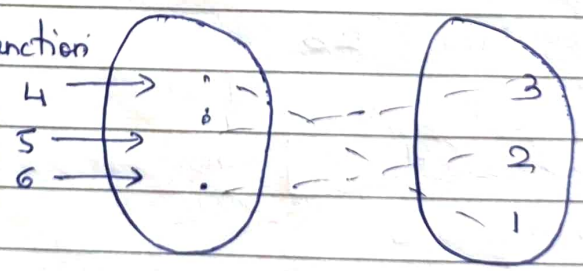


- Feistel Cipher Tech.

Feistel cipher Tech. has three functions or components.

i) Self invertible.
ii) Invertible.
iii) Non-invertible.
iv) Mixer.
v) Swapper.

* Invertible function

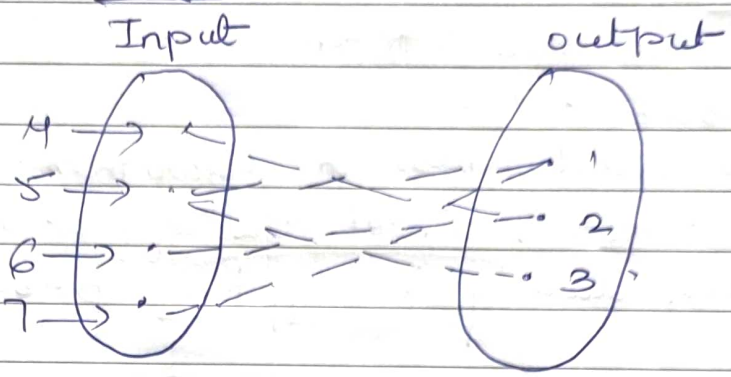


one to one

(456) → (132)

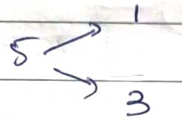
__/__/____

* Non-invertible function:



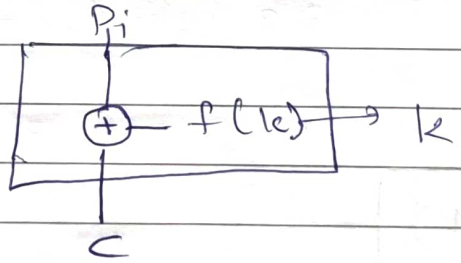
One to many

4 → 2
5 → 1
5 → 3
6 → 2
7 → 1

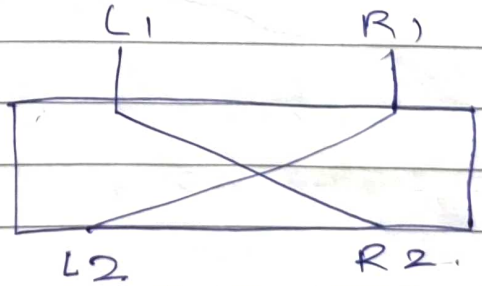


* Self-Invertible:
If function is equal to its inverse is called as self-invertible. i.e. $a == a^{-1}$

* Mixer:



* Swapper:



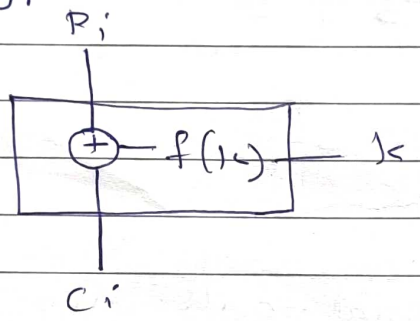
__/__/____

Why X-OR is used?

(1) Does not lose information.
(2) Reversable.
(3) Induce randomness in algorithm.
(4) X-OR function cancel the effect of encryption operation during decryption process.

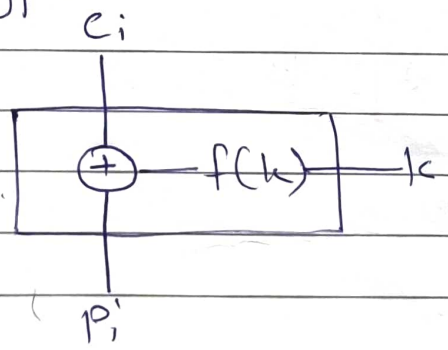
First Draft of Feistel Cipher Tech:

Encryption



$C_i = P_i \oplus f(k)$

Decryption



$P_i = C_i \oplus f(k)$

Ex: p = 0111
f(k) = 1001
C = 0111 ⊕ 1001 = 1110
p = 1110 ⊕ 1001 = 0111

Limitations:

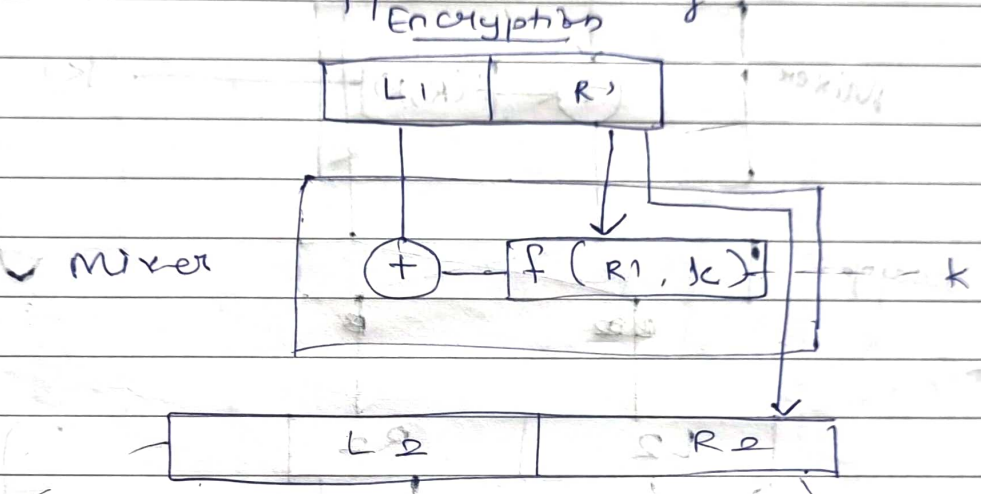
In the first draft of feister cipher Tech is:

① function is applied on key only.

Second Draft of Feistel Cipher Tech.

In second draft of feistel cipher Tech is function is applied on key as well as data.

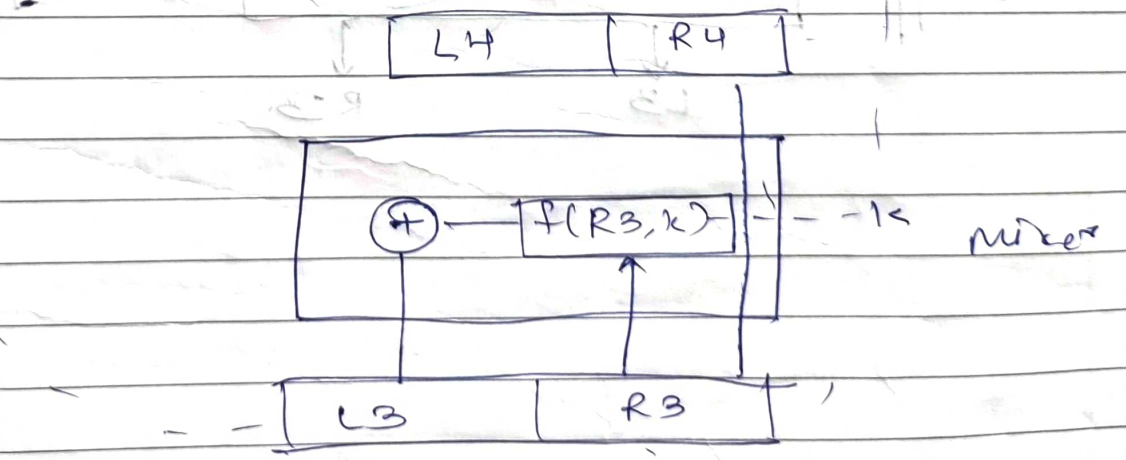
Encryption



$L_2 = L_1 \oplus f(R_1, k)$

$R_2 = R_1$

Decryption:



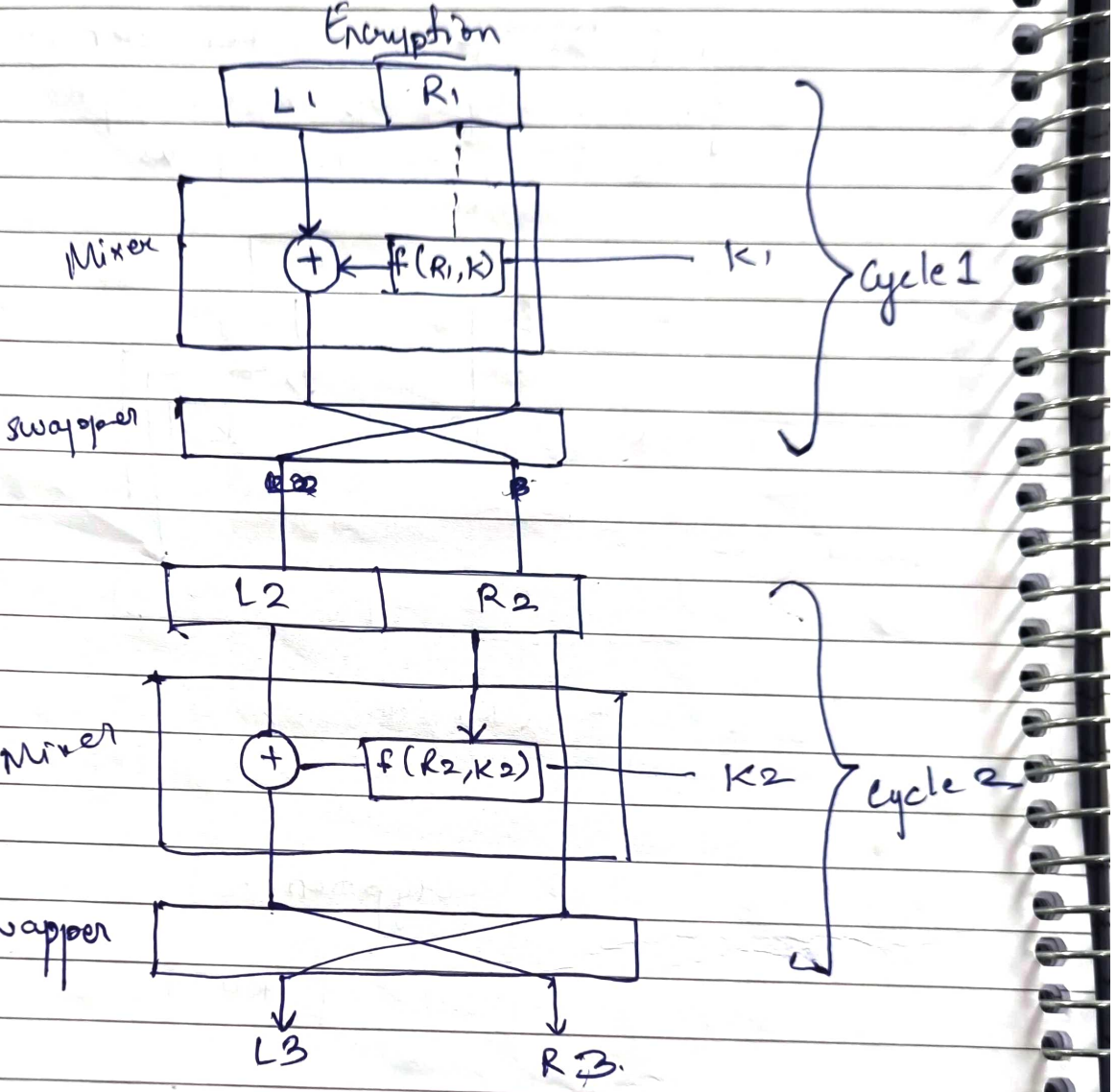
$L_4 = L_3 \oplus f(R_3, k)$

$R_4 = R_3$

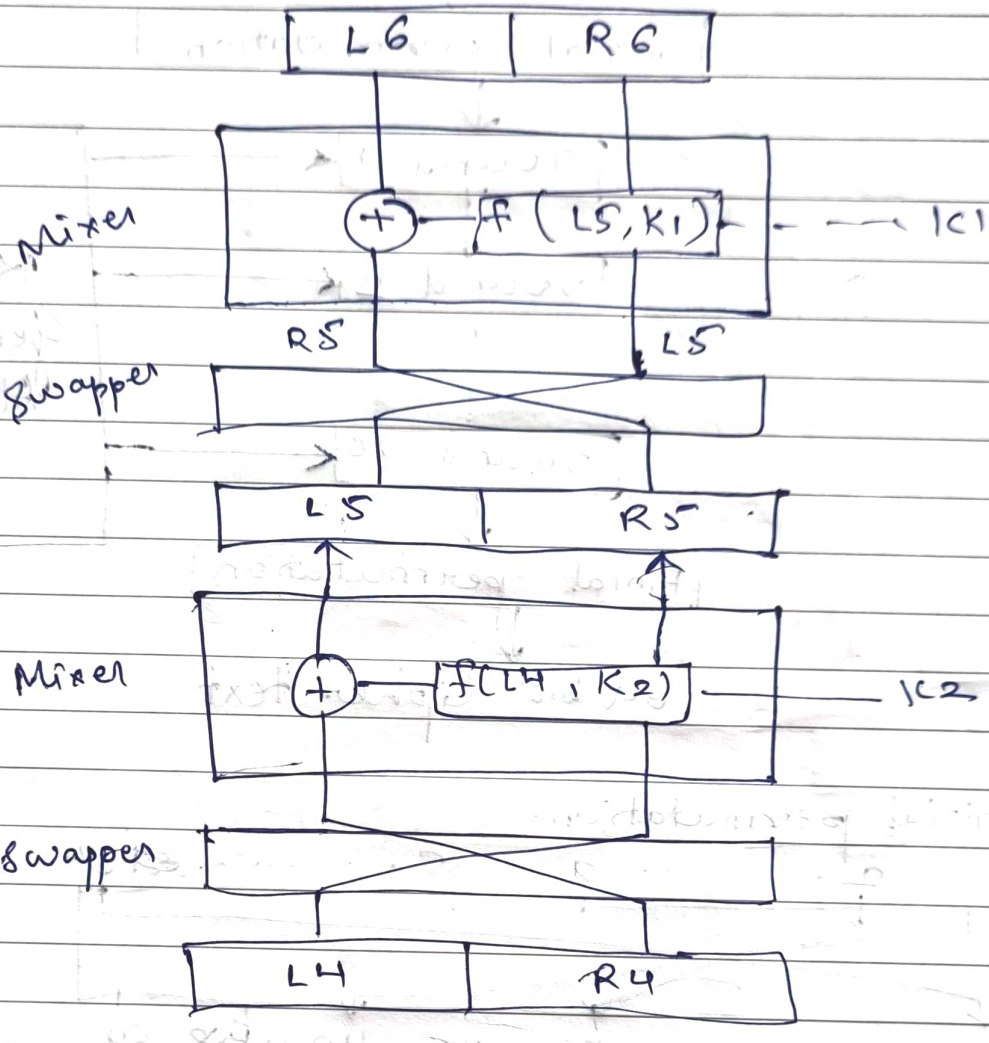
__/__/____

Final Draft of Feistel Cipher

1. Increasing No. of Round.
2. Performing operation on left hand and Right hand side data.



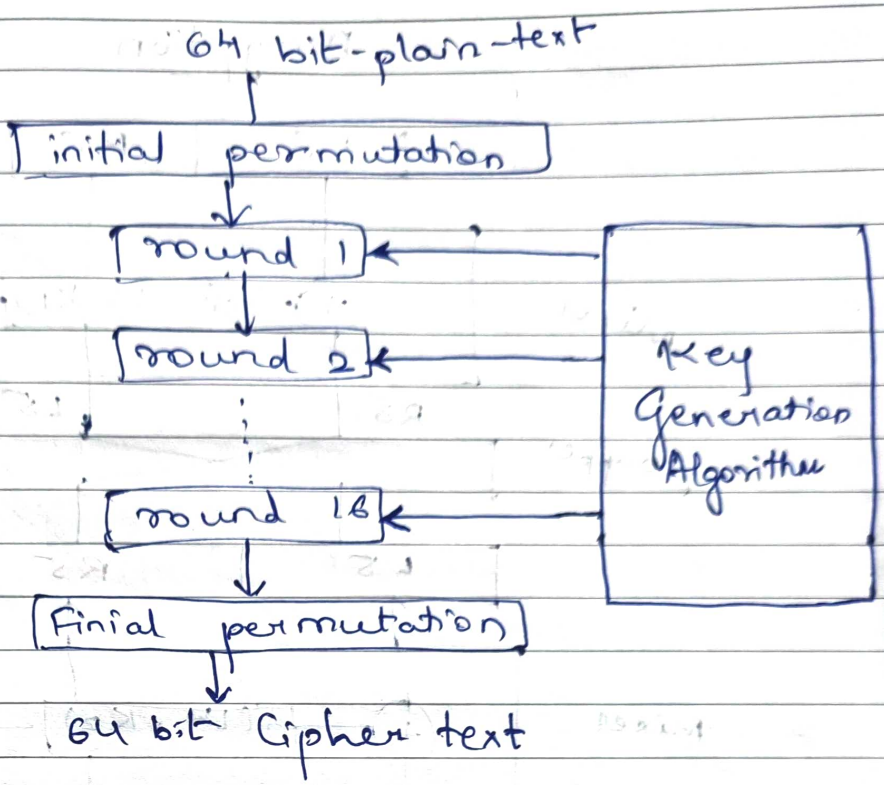
Decryption



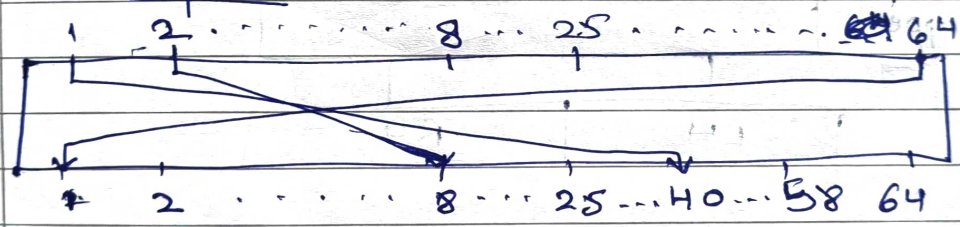
DES algorithm is based on fiesel cipher working principle

* DES Algorithm
  - DES → Data Encryption standards.
  - NIST →
  - DES - March 1975
  - Symmetric Encryption Technology.
  - 16 cycle / 16 - Rounds.
  - 16 keys
  - Brute force attack.
  - S-box - hidden trapdoor.

__/__/____

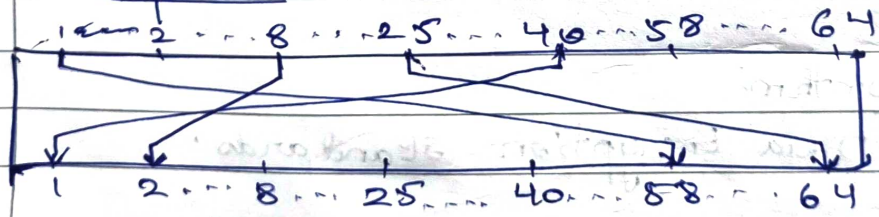


1] Initial permutation:



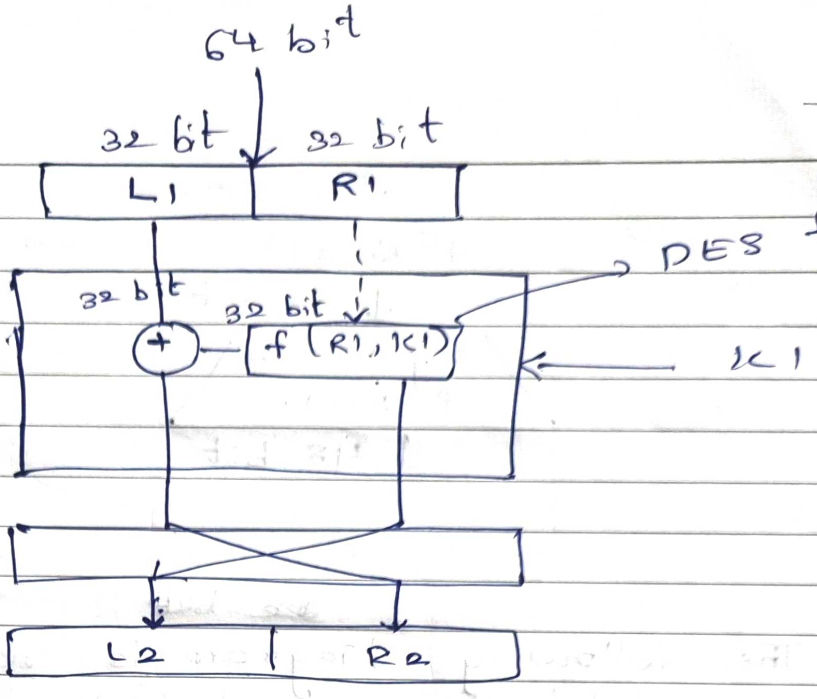
1 → 40
2 → 8
64 → 1

2] Final permutation:

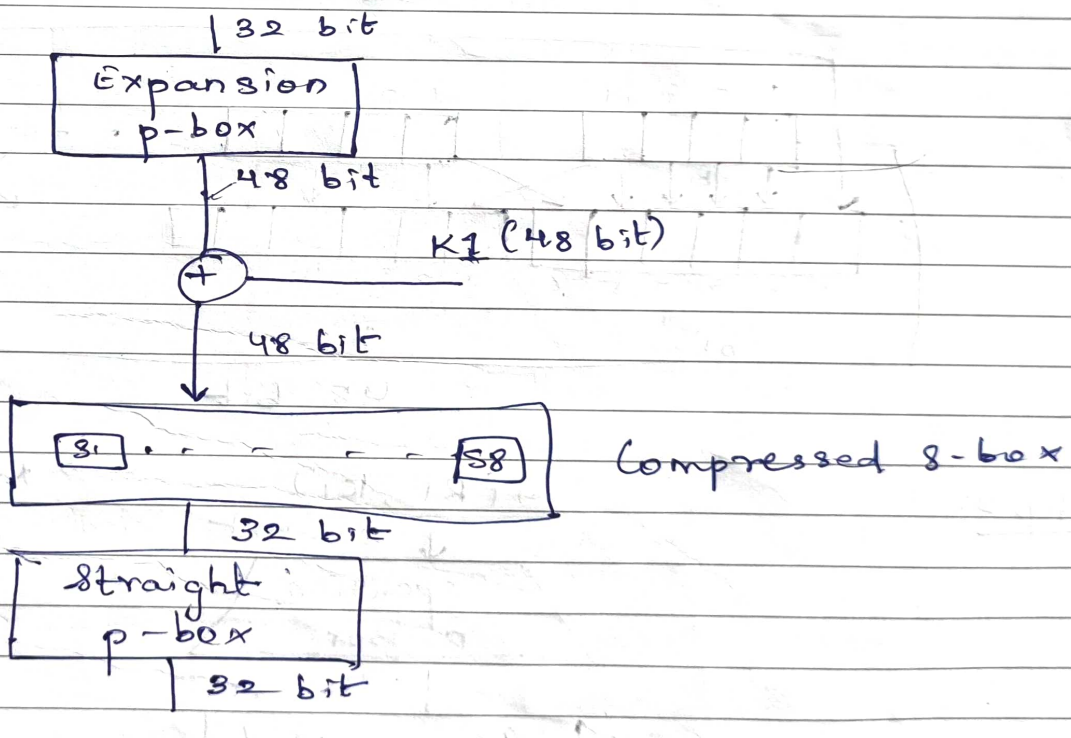


1 → 58
8 → 2
25 → 64
40 → 1

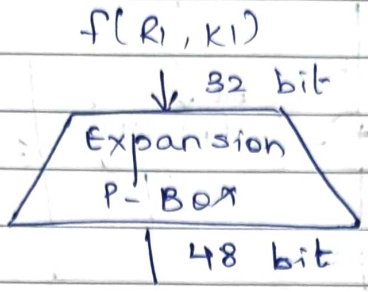
3] Single cycle operation / Single Round operation:



3 :) DES function:

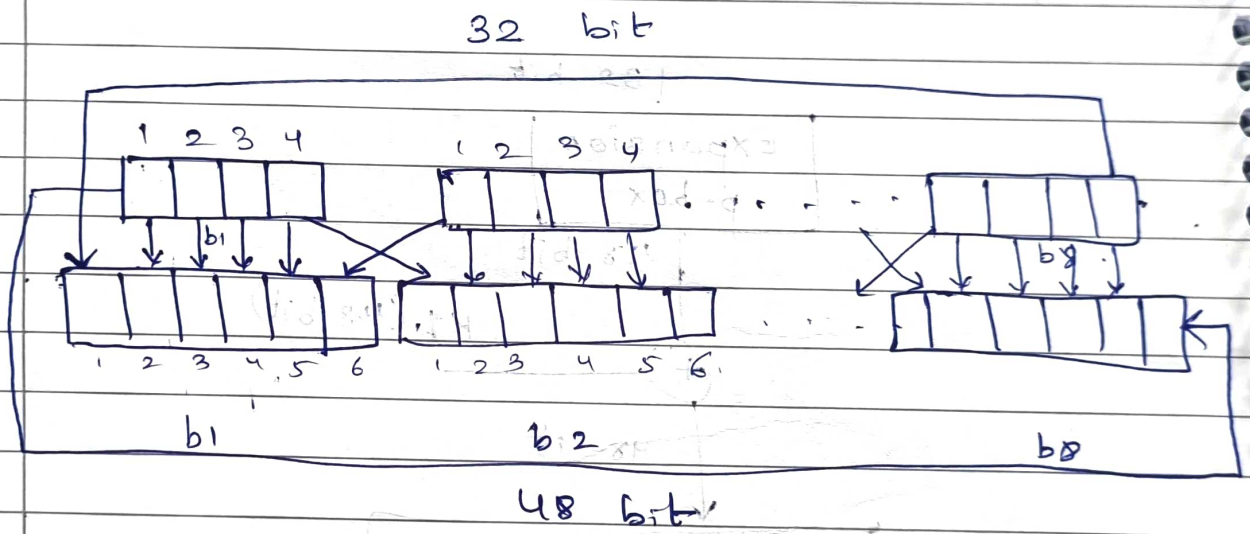


Step 1:

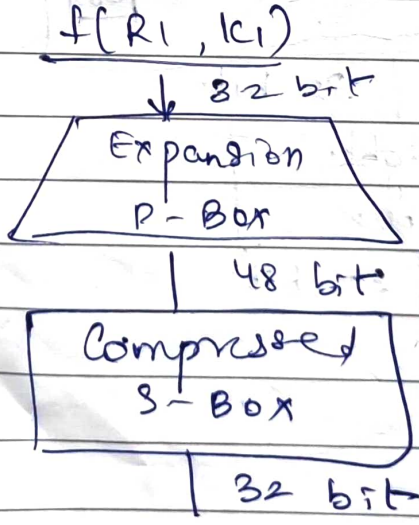


Step 1

The following diagram is represented how 48 bit data is generated from 32 bit data:



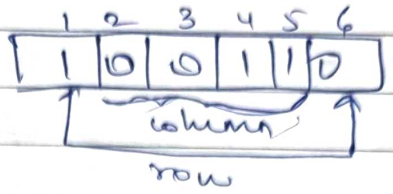
Step 2:



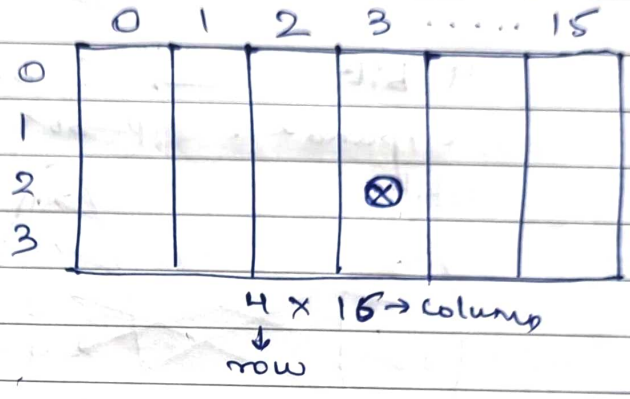
Step 2

Step 2.

48 bit



10 → 2
0011 → 3



Step 3:

f(R1, K1) → Mixer

32 bit

Expansion P-Box — step 1.

48 bit

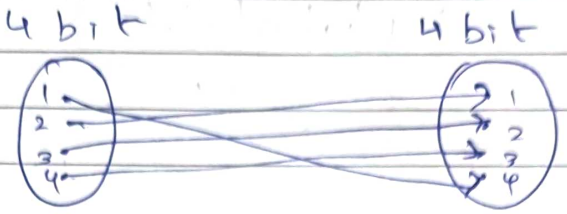
Compressed S-Box — step 2

32 bit

Straight P-Box — step 3.

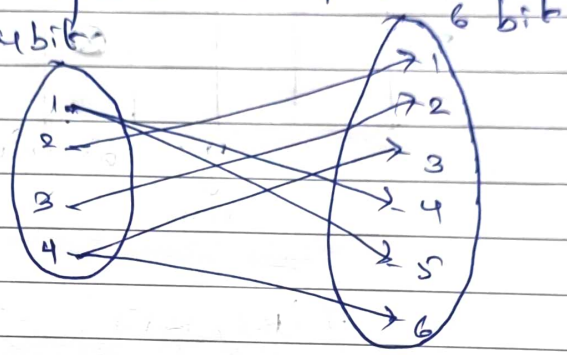
32 bit

straight P-BOX

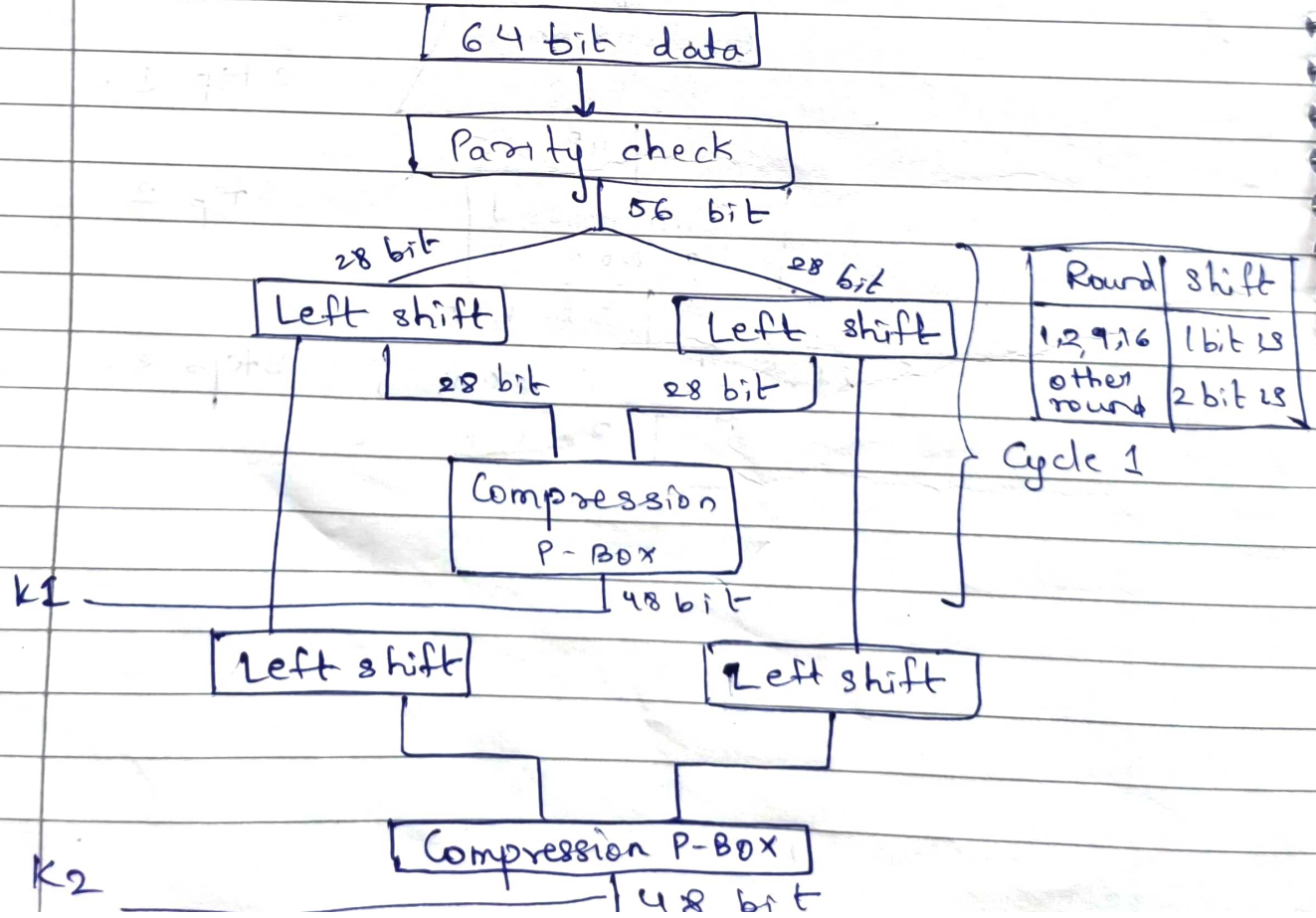


Extra

4 bit → 6 bit.
Expanded P-box



4]. Key Generation Tech./Mechanism in DES.



__/__/____

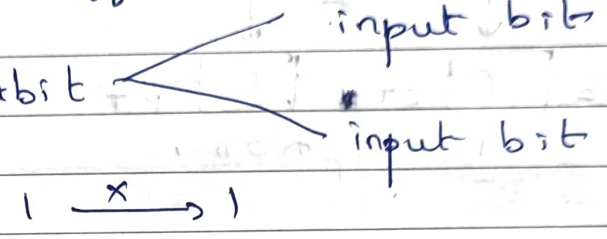
- Properties of DES algorithm:

i) Avalanche effect:
Changes in plaintext affects major change in the cipher text.

input 1 PT = 0000 0000
CT = 4789 2345

input 2 PT = 0000 0001
CT = 3457 #232

ii) Completeness effect:



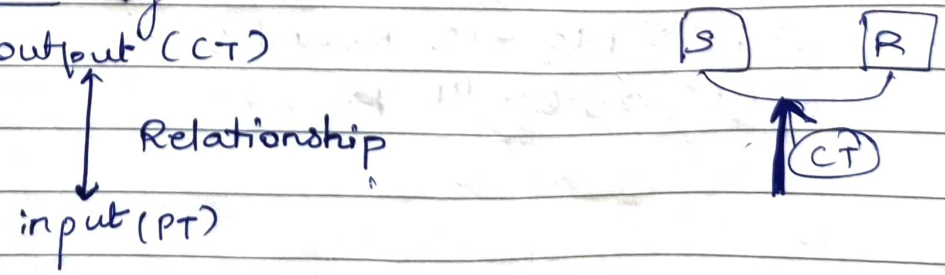
- Security of DES:

i) Brute force attack.
- key
64 bit → parity bits → 56 bits
2^{56} - Attempts.

ii) Deifferential Cryptanalysis:
2.1) Chosen plain text attack.
2.2) Know plain text attack.

DES 2^{47} → Chosen plaintext attacks
2^{55} → Know plaintext attack.

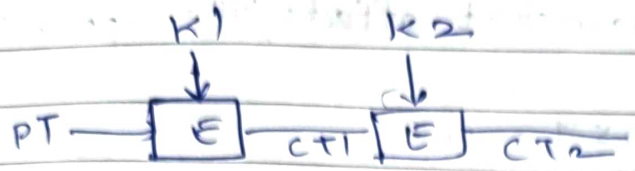
iii) Linear Cryptanalysis:



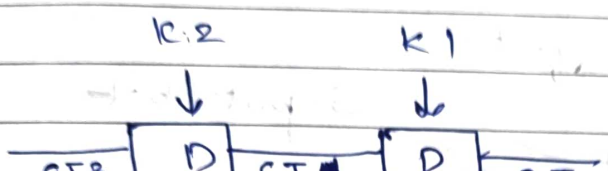
__/__/____

- Double DES:

no of cycles = 32



16 cycle
Encryption

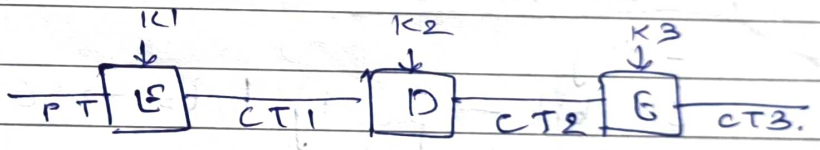


Decryption.

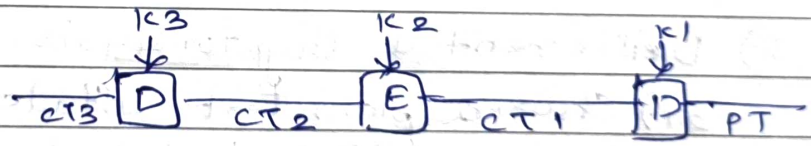
Security of double DES — Forozen.

- Triple DES:

Encryption:
(3-keys)



Decryption:



- AES - Advance Encryption Standards
  - NIST.
  - December 2001.
  - AES
    1. AES 128 - 10 Round. ✓
    2. AES 192 - 12 Round.
    3. AES 256 - 14 Round.

__/__/____

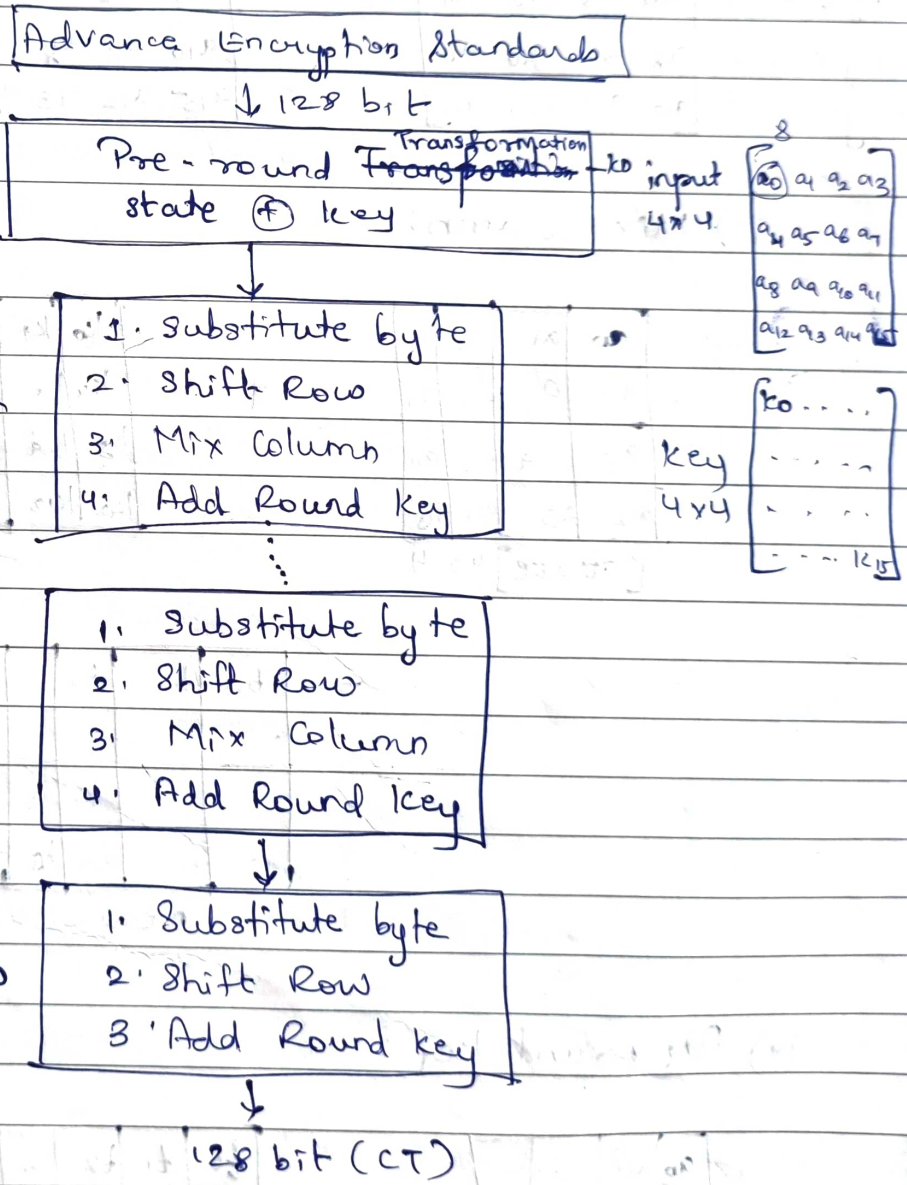
- Applications of AES:

1.) Scandisk:

It is used to protect the data(password). If the password is forgotten then there is no recovery mechanism possible for recovery of password.

ii.) IoS and ipad OS:

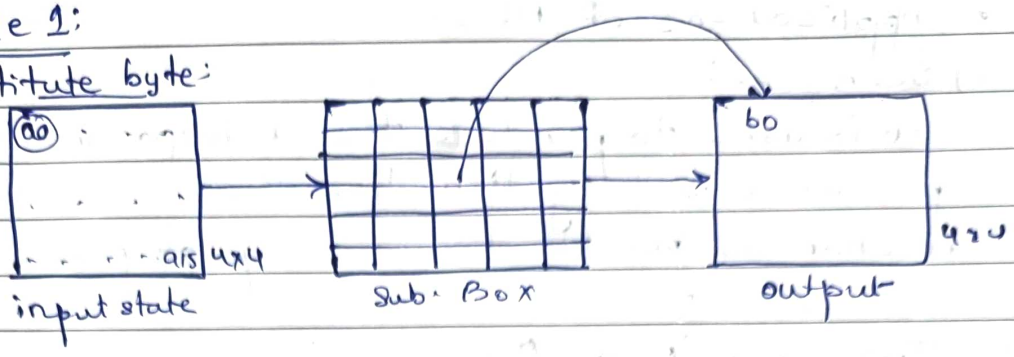
- AES: 128:



__/__/____

Cycle 1:

i) Substitute byte:



ii) Shift Row:

0 byte CLS 1
1 byte CLS 2
2 byte CLS 3
3 byte CLS

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{bmatrix} \xrightarrow{\text{Shift Row}} \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_5 & a_6 & a_7 & a_4 \\ a_{10} & a_{11} & a_8 & a_9 \\ a_{15} & a_{12} & a_{13} & a_{14} \end{bmatrix}$$

iii) Mix Column:

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{bmatrix} * \begin{bmatrix} k_0 & k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 & k_7 \\ k_8 & k_9 & k_{10} & k_{11} \\ k_{12} & k_{13} & k_{14} & k_{15} \end{bmatrix} \rightarrow \text{matrix}$$

[state] 4 x 4 — 4 x 4. — K 4x4 [Matrix].

$$= \begin{bmatrix} b_0 & b_1 & b_2 & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & b_{15} \end{bmatrix}$$

new state [4x4].

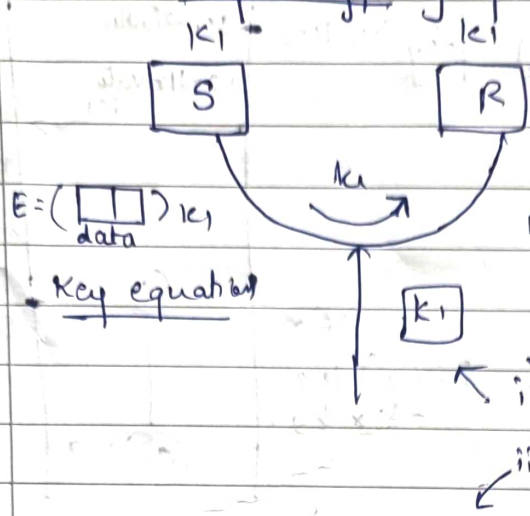
iv) Add Round key:

$$\begin{bmatrix} a_0 & a_1 & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & a_{15} \end{bmatrix} \oplus \begin{bmatrix} t_0 & t_1 & t_2 & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & t_{15} \end{bmatrix} = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & c_{15} \end{bmatrix}$$

state 4x4 — Key [4x4]

__/__/____

- **Public-key Cryptography:**

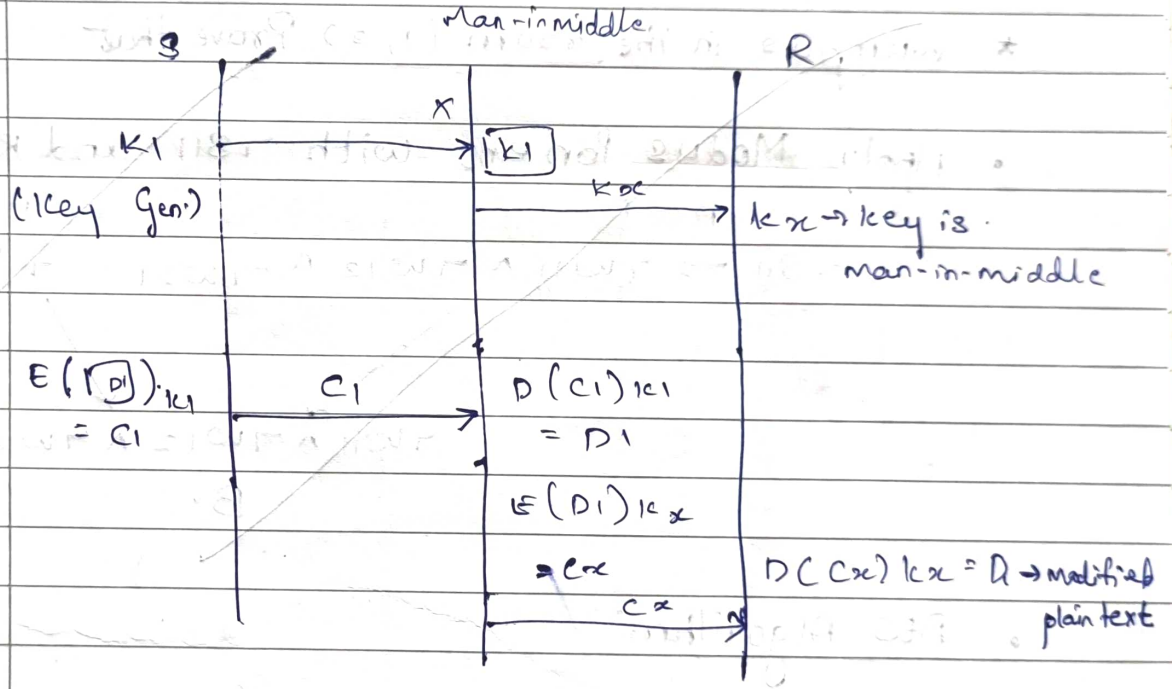


Issues with Symmetric Key Cryptography:

Key equation

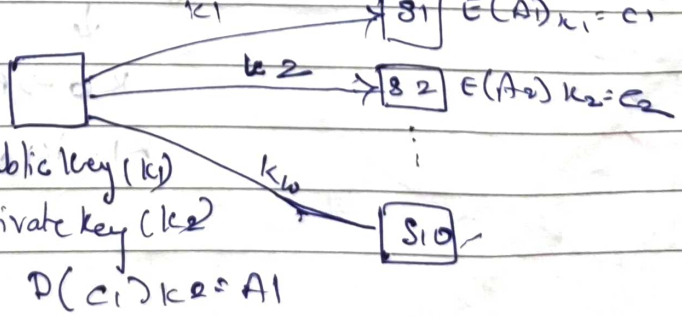
i) Interception + Cryptanalysis

ii) Man-in-middle attack.



The above issue can be partially solved by public-key cryptography.

Public key
Private key.



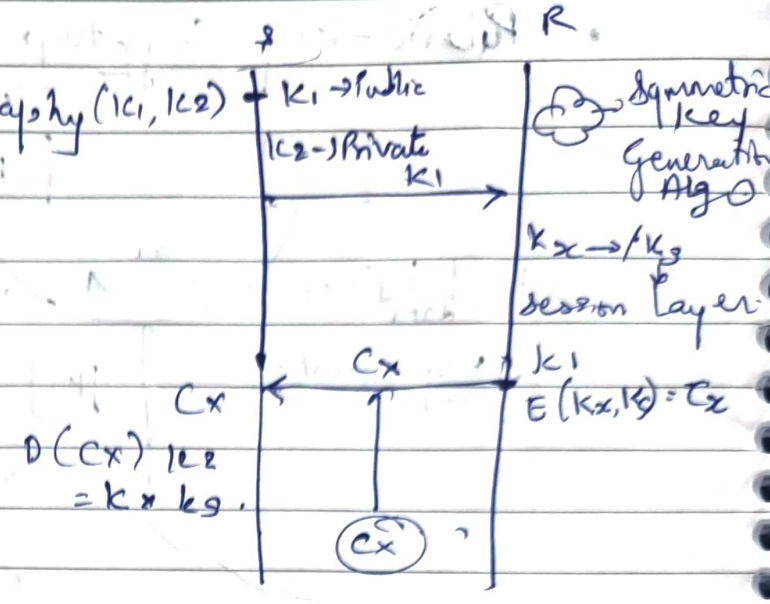
SSL
↳ RSA-1028
RSA-2056.

RSA

Proof → Public key (K1)
Private key (K2)
D(C1)K2 = A1

__/__/____

- Public key Cryptography (k1, k2)
- Symetric key.



* Wumpus in the room (1, 3) Prove that

- Apply Modus Ponens with ¬S11 and R1

A → B

¬S11 → ¬W11 ∧ ¬W12 ∧ ¬W21

A

¬S11

¬W11 ∧ ¬W12 ∧ ¬W21

B.

- AES Algorithm:

Pre Round Transformation
state ⊕ key

state → 4 * 4

key → 4 * 4

AES - Round 10 → key → 11

↓

K0 → Pre Round transformation

K1 - K10 → Round 1 - Round 10

state [A B C D E F . . . . . . P]

4*4 = state = s =

$$\begin{bmatrix} A & E & I & M \\ B & F & J & N \\ C & G & K & O \\ D & H & L & P \end{bmatrix}$$

key (4*4) : K0

$$\begin{bmatrix} D & N & I & C \\ J & G & C & O \\ S & H & O & M \\ A & V & E & P \end{bmatrix}$$

$R_0 = S_0 \oplus K_0$

Alphabet	Hex	Alphabet	Hex
A	00	U	14
B	01	V	15
C	02	W	16
D	03	X	17
E	04	Y	18
F	05	Z	19
G	06		
H	07		
I	08		
J	09		
K	0A		
L	0B		
M	0C		
N	0D		
O	0E		
P	0F		
Q	10		
R	11		
S	12		
T	13		

Note:
All the characters in the state as well as key need to be considered as uppercase.

Hex to Binary

	8	4	2	1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
A	1	0	1	0
B	1	0	1	1
C	1	1	0	0
D	1	1	0	1
E	1	1	1	0
F	1	1	1	1

$R_0 = S_0 \oplus K_0$

$= A \oplus D$

$= 00 \oplus 03$

$= 0000\ 0000 \oplus 0000\ 0011$

$= 0000\ 0011$

$= 03$

$= D$

- KEY EXPANSION / GENERATION IN AES-128 bit:

$$K_0 = \begin{bmatrix} W_0 & W_1 & W_2 & W_3 \\ b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

$w_4\ w_5\ w_6\ w_7$

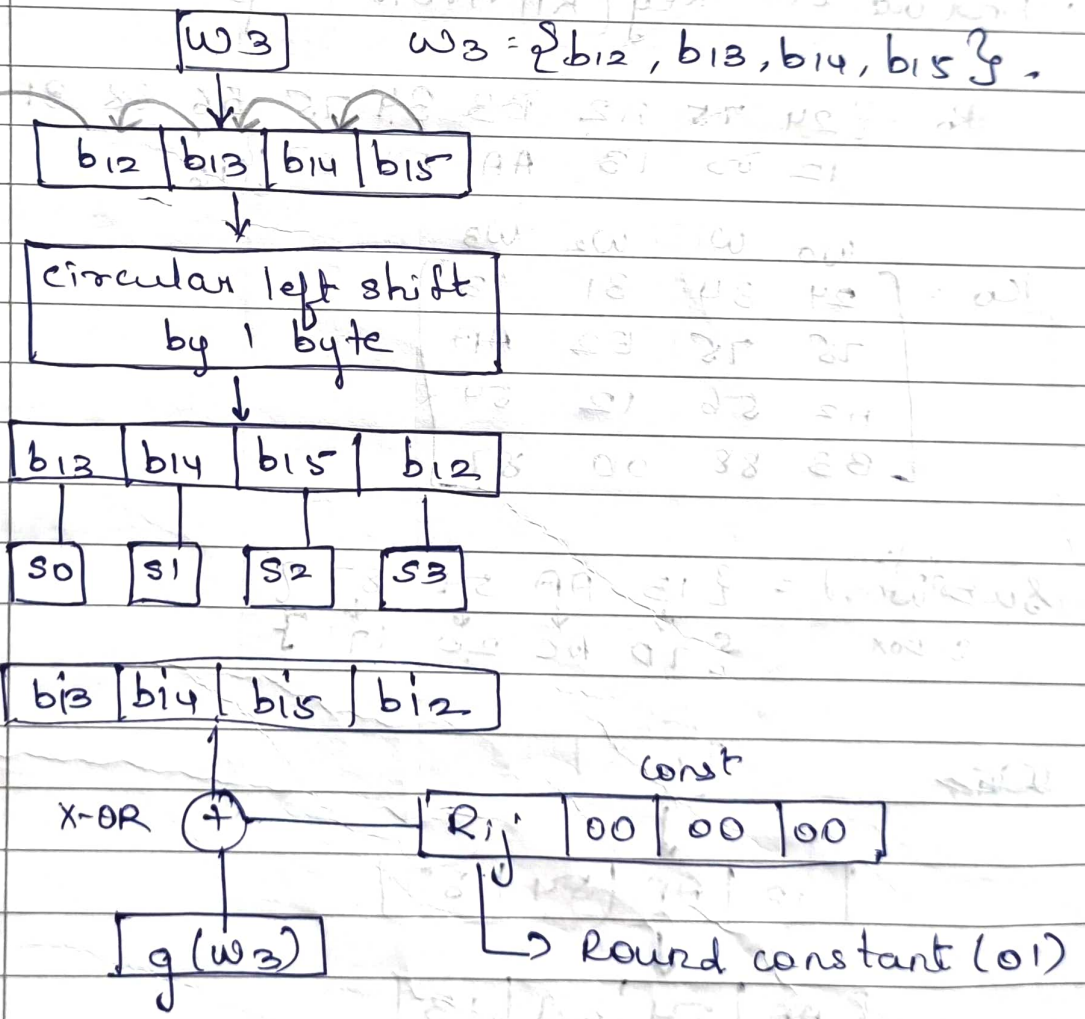
$k_1 = [\ \ \ ]$

$w_4 = w_0 \oplus g(w_3)$
$w_5 = w_1 \oplus w_4$
$w_6 = w_2 \oplus w_5$
$w_7 = w_3 \oplus w_6$

imp

$g(w_3)$

$w_3 = \{b_{12}, b_{13}, b_{14}, b_{15}\}$.



__/__/____

Round constant:

R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}
(Round)									
01	02	04	08	10	20	40	80	1B	36

R(ij)

$Rc_i = x^{i-1} \bmod prime$

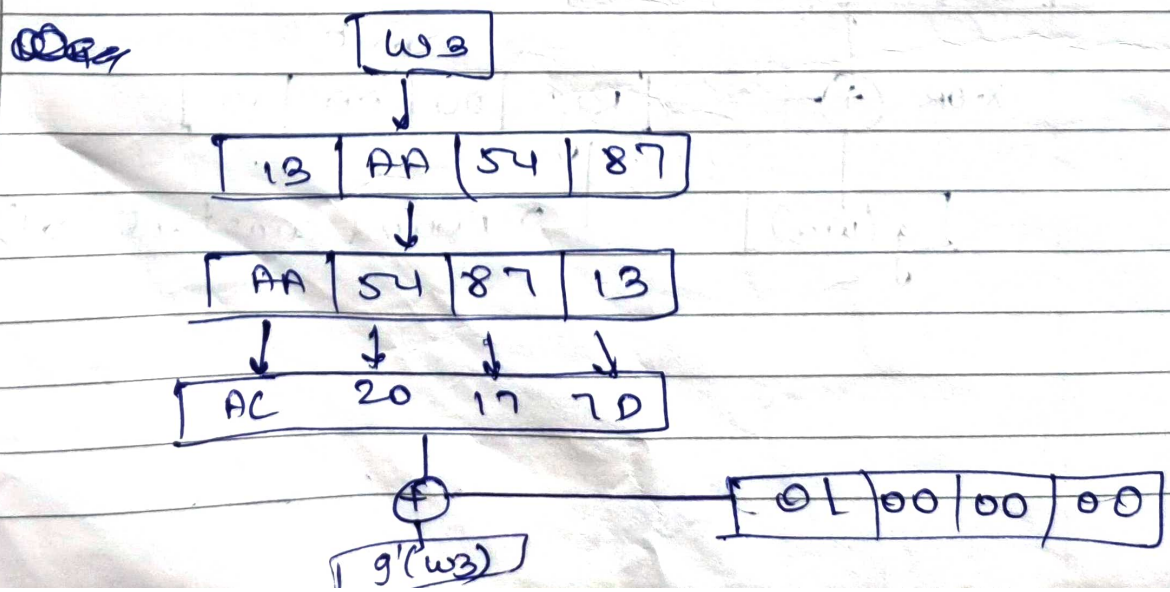
$Rc_1 = x^{1-1} \bmod prime = 1 = (01)_{16}$

Q. Find out the key (k_1) from key (k_0).

$k_0 = \{24\ 75\ A2\ B3\ 34\ 75\ 56\ 88\ 31\ E2\ 12\ 00\ 13\ AA\ 54\ 87\}_{16}$

$$k_0 = \begin{bmatrix} W_0 & W_1 & W_2 & W_3 \\ 24 & 34 & 31 & 13 \\ 75 & 75 & E2 & AA \\ A2 & 56 & 12 & 54 \\ B3 & 88 & 00 & 87 \end{bmatrix}$$

Substitution Word = $\{13\ AA\ 54\ 87\}$
S-Box $\{7D\ AC\ 20\ 17\}$



__/__/__

$t_0 = AC \oplus 01$

$= 1010\ 1100 \oplus 0000\ 0001$

$= 1010\ 1101$

$t_0 = AD$

$t_1 = 20 \oplus 00$

$= 0010\ 0000 \oplus 0000\ 0000$

$= 0010\ 0000$

$t_1 = 20$

$t_2 = 17 \oplus 00$

$= 0001\ 0111 \oplus 0000\ 0000$

$= 0001\ 0111$

$t_2 = 17$

$t_3 = 7D \oplus 00$

$= 0111\ 1101 \oplus 0000\ 0000$

$= 0111\ 1101$

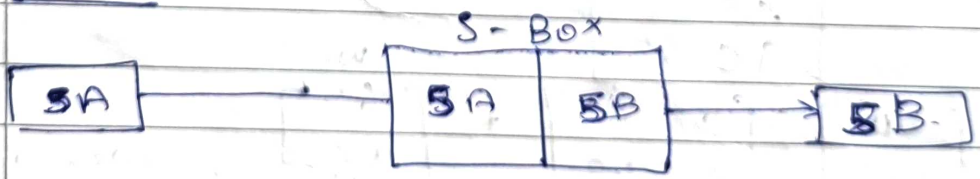
$t_3 = 7D$

incomplete

AES

Mix Columnar updation

Sub



Intrabyte Changes

$(5A)_{16}$

0101 1010.

intrabyte changes

__/__/____

State (4×4) :

w_0	w_1	w_2	w_3
b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

4×4

Constant Matrix 1 byte CR ____ 1 byte CR ____ 1 byte CR ____

$$C = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad (w_0' = C * w_0)$$

Note: Also generate w_1', w_2', w_3' as w_0'

Note:

Eg: 2×2 Const matrix $2 \times 2 = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix}$

Eg:

State : w_0 w_1

$$\begin{bmatrix} 63 & 47 \\ 9C & 63 \end{bmatrix}$$

w_0'

$$\begin{bmatrix} b_0' \\ b_1' \end{bmatrix} = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix} * \begin{bmatrix} 63 \\ 9C \end{bmatrix} \quad (w_0)$$

Hex value → Hex value

$= (02 * 63) \oplus (03 * 9C)$

↳ finite field Arithmic operation

ie. $GF(2^8)$

↳ Galian field

__/__/____

(02) = 0000 0010
(63) = 0110 0011

GF(2^8) = $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
{0000 0000 . — — — — — — — — 1111 1111}.

(02) = 0 0 0 0 0 0 1 0
= x

(63) = 0 1 1 0 0 0 1 1
= $x^6 + x^5 + x + 1$

= $x * (x^6 + x^5 + x + 1)$
= $x^7 + x^6 + x^2 + x$
= 1100 0110
= C6 (02 * 63)

(03) = 0000 0011
(9c) = 1001 1100

(03) = 0 0 0 0 0 0 1 1
= $x + 1$

(9c) = 1 0 0 1 1 1 0 0
= $x^7 + x^4 + x^3 + x^2$

= $(x+1)(x^7 + x^4 + x^3 + x^2)$
= $x(x^7 + x^4 + x^3 + x^2) + 1(x^7 + x^4 + x^3 + x^2)$
= $x^8 + x^5 + x^4 + x^3 + x^7 + x^4 + x^3 + x^2$
$s(x) = x^8 + x^7 + x^5 + x^2$ (03 * 9c)

The above polynomial is not a part of GF(2^8) form.

Use irreducible polynomial form to convert it in GF(2^8) form.

$p(x) = x^8 + x^4 + x^3 + x + 1$ → w_0 given

$t(x) = \frac{s(x)}{p(x)}$

$s(x) = 110100100$

(x^8 x^7 x^6 x^5 x^4 x^3 x^2 x^1 x^0)

$p(x) = 100011011$

```
100011011 | 110100100
           - 100011011
           -----------
             010111111
                B    F   — (03 * 9C)
```

w_0' = C6 ⊕ BF

= 1100 0110 ⊕ 1011 1111

= 0111 1001

= 79

(01 * 63) + (02 * 9C)

(01) = 0000 0001 = 1

(63) = 0110 0011 = $x^6 + x^5 + x + 1$

$x^6 + x^5 + x + 1$

$= 0110\ 0011$

$= 6\ 3$

$(02) = 0000\ 0010 = x$

$(ac) = 1001\ 1100 = x^7 + x^4 + x^3 + x^2$

$x * (x^7 + x^4 + x^3 + x^2)$

$= x^8 + x^5 + x^4 + x^3$

$s(x) = 100111000$

$$
\begin{array}{r|l}
100011011 & 100111000 \\
 & -\ 100011011 \\
\hline
 & 000100011 \\
 & \quad 2\quad 3
\end{array}
$$

$= 63 \oplus 23$

$= 0110\ 0011 \oplus 0010\ 0011$

$= 0100\ 0000$

$= 4\ 0$

- Knapsack Cryptosystem:
  - Public key cryptography
  - Markel - Hellmen.

Knapsack:

$a_x = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$.

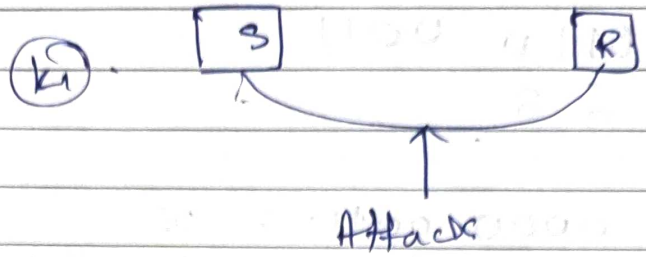
input $= \{150, 180, 170, 200, 280, 300, 520, 270\}$.

Target $s = 950$ gms.

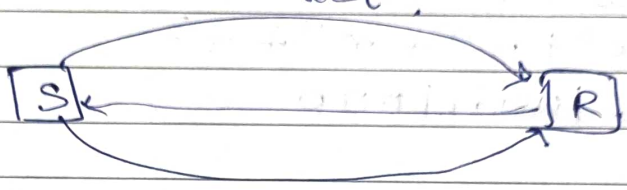
$x = \{a_1, a_5, a_6, a_6\}$,

output $150 + 200 + 300 + 300 = 950$.

__/__/____



Public



- Private key will be given.

Private key = $\{a_1, a_2, a_3, a_4\} = S_i$

Step 1:

$a_2 > a_1$

$a_3 > a_1 + a_2$

$a_4 > a_1 + a_2 + a_3$

Super increased sequence

Step 2: Private key = ?

n

m

↳ $m > \{a_1 + a_2 + a_3 + a_4\}$

↳ n value should be relatively prime to m.

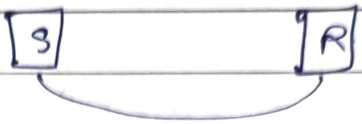
$GCD(n, m) = 1$

Step 3: $S_i * n \bmod m$

$S_i \rightarrow$ Super increased sequence

$i = 1$ to n.

Public key = $\{b_1, b_2, b_3, b_4\}$.



$\{a_1, a_2, a_3, a_4\}$ → Private.

↓

$\{b_1, b_2, b_3, b_4\}$ → Public.

Ex:8. Bob want to share the following 8 bit message with Alice in secret manner using following keys:

Soln: 8 bit message

1100 0011

Alice Private key {1, 2, 4, 10}.

Soln: Alice public key

$m > 1+2+4+10$

$20 > 17$

$m = 20$ $n = ?$

$n = 7$ $GCD(n, m) = 1$

$3; \ast n \bmod m$

$1 * 7 \bmod 20 = 7$

$2 * 7 \bmod 20 = 14$

$4 * 7 \bmod 20 = 8$

$10 * 7 \bmod 20 = 10$

Alice public key = {7, 14, 8, 10}

Alice public key is shared with Bob.

Encryption

$1100 = 1*7 + 1*14 + 0*8 + 0*10 = 7 + 14 = 21$

$0011 = 0*7 + 0*14 + 1*8 + 1*10 = 8 + 10 = 18$

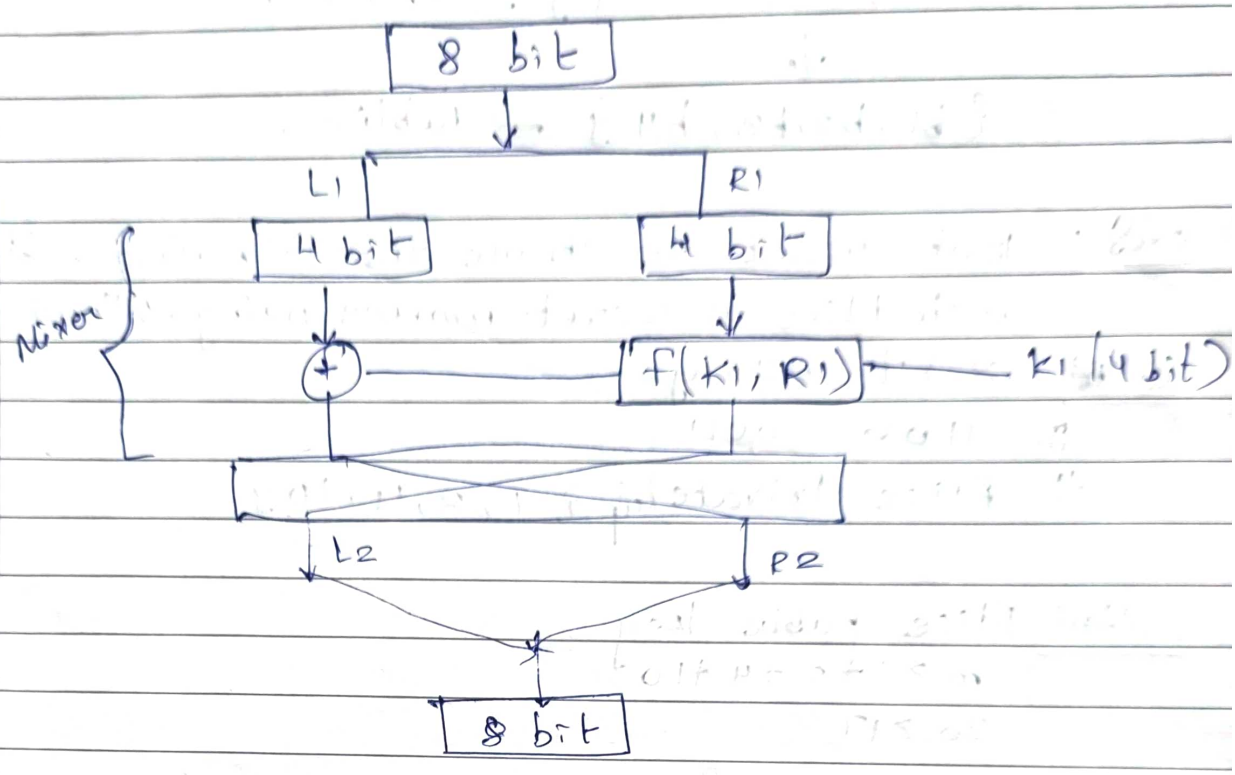
CT = 21

CT : 18

__/__/__

Exp: 6

Aim: Implement simplified DES algorithm:



Exp 4:

plaintext
Key
5x5 matrix, display
Ciphertext

} Code

__/__/____

Exp 3.

Aim: Implement Affine Cipher Tech. (Convert Plaintext into cipher text).

Theory: 3-4 lines about Introduction to Affine Cipher Tech.

Algorithm

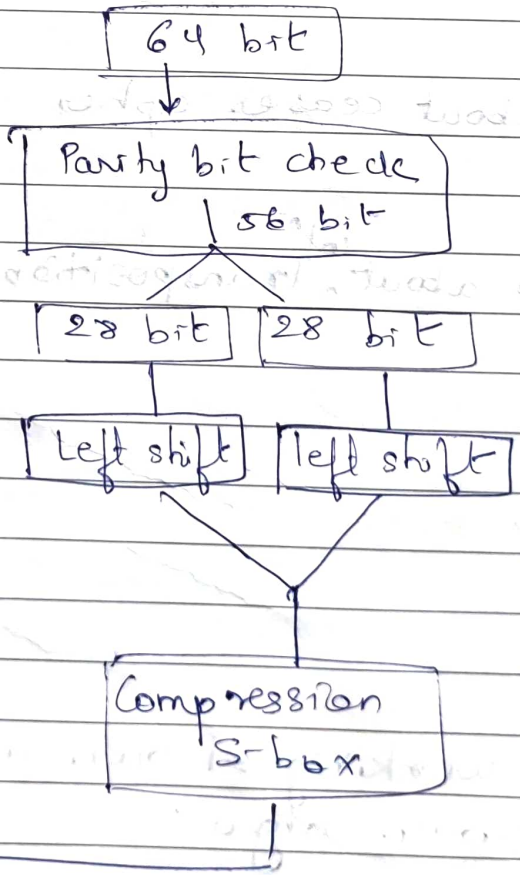
Example:

#code

#output of program.

Exp 5.

Aim: Implement DES Single Key Generation Tech.



- **Decryption**

CT: 21 18

n = 7

$n \times n^{-1} \bmod m = 1$

$7 \times n^{-1} \bmod 20 = 1$

$1 \times 7 \bmod 20 = 7$

$2 \times 7 \bmod 20 = 14$

$3 \times 7 \bmod 20 = 1$

$n^{-1} = 3$

$(21 \times 3) \bmod 20 = 3$

Private key = {1, 2, 4, 10}.

1100

$(18 \times 3) \bmod 20 = 14$

Private key = {1, 2, 4, 10}

0011

Ex Q2. Convert plaintext into cipher text and vice versa using following input and private key.
Private key = {2, 3, 7, 14}.
input : 1101 0101

Soln: ~~Private~~ public key.

$m > 2+3+7+14$

$30 > 26$

$m = 30$

$n = 7$ $\quad gcd(n, m) = 1$

Si * n mod m
2 * 7 mod 30 = 14
3 * 7 mod 30 = 21
7 * 7 mod 30 = 19
14 * 7 mod 30 = 8

public key = {14, 21, 19, 8}

Encryption

1101 = 1*14 + 21*1 + 0*19 + 1*8 = 14 + 21 + 8 = 43

0101 = 0*14 + 1*21 + 0*19 + 1*8 = 21 + 8 = 29

CT = 43 29

Decryption

CT = 43 29

n = 7

$n * n^{-1} \bmod m = 1$

$7 * n^{-1} \bmod 30 = 1$

1 * 7 mod 30 = 7
2 * 7 mod 30 = 14
3 * 7 mod 30 = 21
4 * 7 mod 30 = 28
5 * 7 mod 30 = 5
6 * 7 mod 30 = 12
7 * 7 mod 30 = 19
8 * 7 mod 30 = 26
9 * 7 mod 30 = 03
10 * 7 mod 30 = 10
11 * 7 mod 30 = 17
12 * 7 mod 30 = 24

13 * 7 mod 30 = 1

__/__/__

Rough

$(43 * 13) \bmod 30 = 19$

Private key = {2, 3, 7, 14}

1 1 0 1

$(29 * 13) \bmod 30 = 17$

Private key = {2, 3, 7, 14}

0 1 0 1

★ RSA Algorithm:

- Public key cryptography.
- p, q → multiplication = n.
  - two prime no.
  - $n = p * q$
    - ↳ factorization
- SSL - RSA
  - → 1024 bit
  - → 2048 bit

Steps:

i) Select two prime numbers p, q

ii) $n = p * q$

iii) Euler totient function
$\phi(n) = (p-1) * (q-1)$

iv) Find out value of e ?
e ← Relatively Prime to → $\phi(n)$
$\gcd(e, \phi(n)) = 1$

v) Find out value of d ?
$(e * d) \bmod \phi(n) = 1$

vi) Encryption

Rough

43
*13
129

43*
559

18
30)559
-30
259
-240
019

29
*13
187
29*
377

12
30)377
-30
077
-60
17

Euler totient function

$\phi(10)$
10 → 2, 5

$\phi(1)$, $\phi(2)$
$\phi(3)$, $\phi(4)$,
$\phi(5)$, $\phi(6)$
$\phi(7)$, $\phi(8)$
$\phi(9)$, $\phi(10)$

$\phi(10) = 4$

M → Message

$C = M^e \bmod n$ (e, n)

viii) Decryption

$M = c^d \bmod n$ (d, n)

Example:

Q. $p = 3, q = 5$

$M = 4$ (Plain text)

Soln: 1) $n = p * q$

$= 3 \times 5$

$n = 15$

2) $\phi(n) = (3-1) * (5-1)$

$= 2 \times 4$

$\phi(n) = 8$

3) $e = ?$

$e = 3$

public key (3, 15)

4) $d = ?$

$(d * e) \bmod \phi(n) = 1$

$(1 * 3) \bmod 8 = 1$

$(2 * 3) \bmod 8 = 1$

$(3 * 3) \bmod 8 = 1$

$d = 3$

private key (3, 15)

5) $C = M^e \bmod n$

$= 4^3 \bmod 15$

$= 64 \bmod 15$

$C = 4$

6) $M = c^d \bmod n$

$= 4^3 \bmod 15$

$= 64 \bmod 15$

$M = 4$

Q. Using RSA Algo. find out following

a) public key? 2.) Private key.

3.) Perform Encryption of input value M = 3)

4.) Perform Decryption of cipher text

$p = 3, q = 11$

Soln: 1.) $n = p * q$

$= 3 \times 11$

$n = 33$

2.) $\phi(n) = (3-1) * (11-1)$

$= 2 * 10$

$\phi(n) = 20$

3) $e = ?$

$e = 3$

public key (3, 33)

4.) $d = ?$

$(d * e) \bmod \phi(n) = 1$

$(1 * 3) \bmod 20 \neq 1$

$(2 * 3) \bmod 20 \neq 1$

$(3 * 3) \bmod 20 \neq 1$

$(4 * 3) \bmod 20 \neq 1$

$(5 * 3) \bmod 20 \neq 1$

$(6 * 3) \bmod 20 \neq 1$,

$(7 * 3) \bmod 20 = 1$,

$d = 7$

(7, 33) → private key.

216 / 4 = 64

184955018

Ans → Before value

__/__/____

5.) $C = M^e \bmod n$

$= 31^3 \bmod 33$

$= 29791 \bmod 33$

$C = 25$

6.) $M = c^d \bmod n$

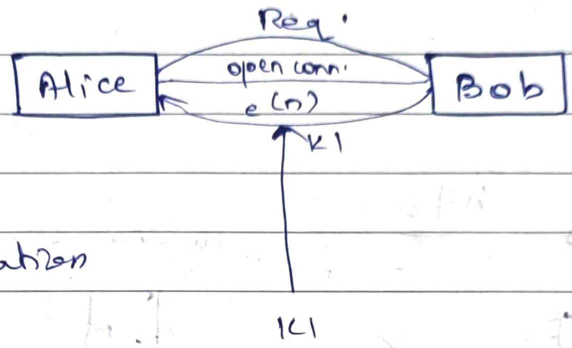
$= 25^7 \bmod 33$

$= 6103515625 \bmod 33$

$M = 31$

Attacks on RSA:

i.) Factorization Attack:



E (K1)

AES generation

Public key = (e, n)

Private key (d, n)

D(Cx) key = K1

Symmetric + public key

Alice | | | Bob

x p, q

n, $\phi(n)$

public key (e, n)

private key (d, n)

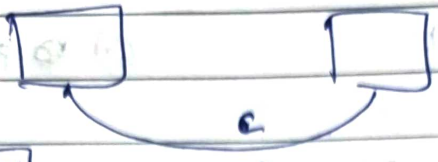
- Plaintext Attack:-

a.) Short Message Attack:

4 bit → 0000

⋮

Cryptanalysis. 9999



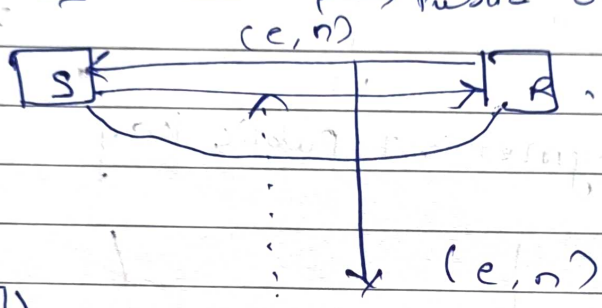
$C = M^e \bmod n$ → c 4 digit.

Attacker Interruption.

$d_1 (e, n)$ → 0000 → m1 ... 9999

$c_1 = (M)^e \bmod n$,

ii) Cycling Attack:-



$E([M])_{(e,n)}$ → c_1 → cipher text

$C = M^e \bmod n$

$c_2 = c_1^e \bmod n$,

$c_3 = c_2^e \bmod n$

$c_4 = c_3^e \bmod n$

$\vdots$

$c_k = c_{k-1}^e \bmod n$;

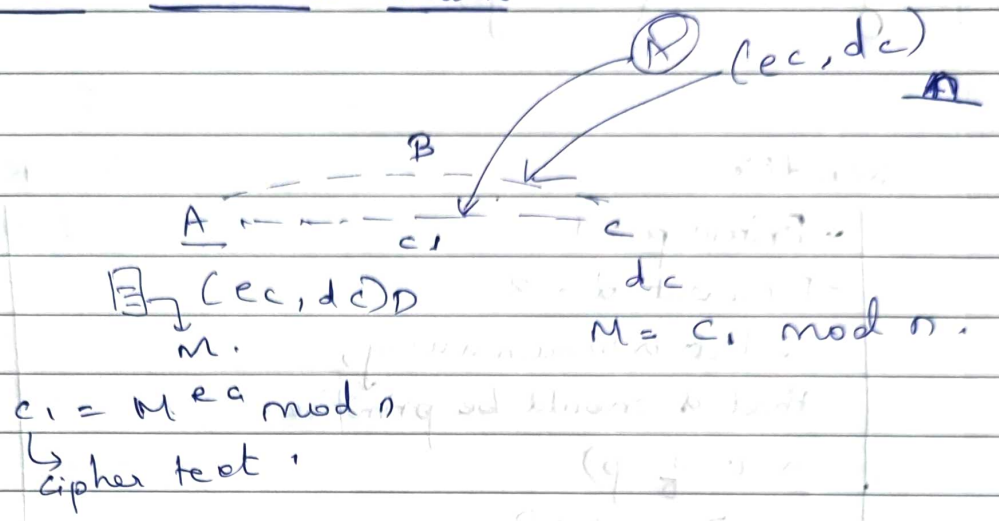
$c_1 \neq c_k$.

iii) Unconcealed Message Attack:-

When the ciphertext is equal to the original plaintext then it is called as unconcealed message Attack.

Attack on the Modulus:

(a:) **Common Modulus attack:-**



Attack on Implementation

Timing Attack:-

Prevention Guideline for RSA attack:-

1.) The number of bits for n should be atleast 1024. This means that n should be around 2^{1024} or 309 decimal digit.

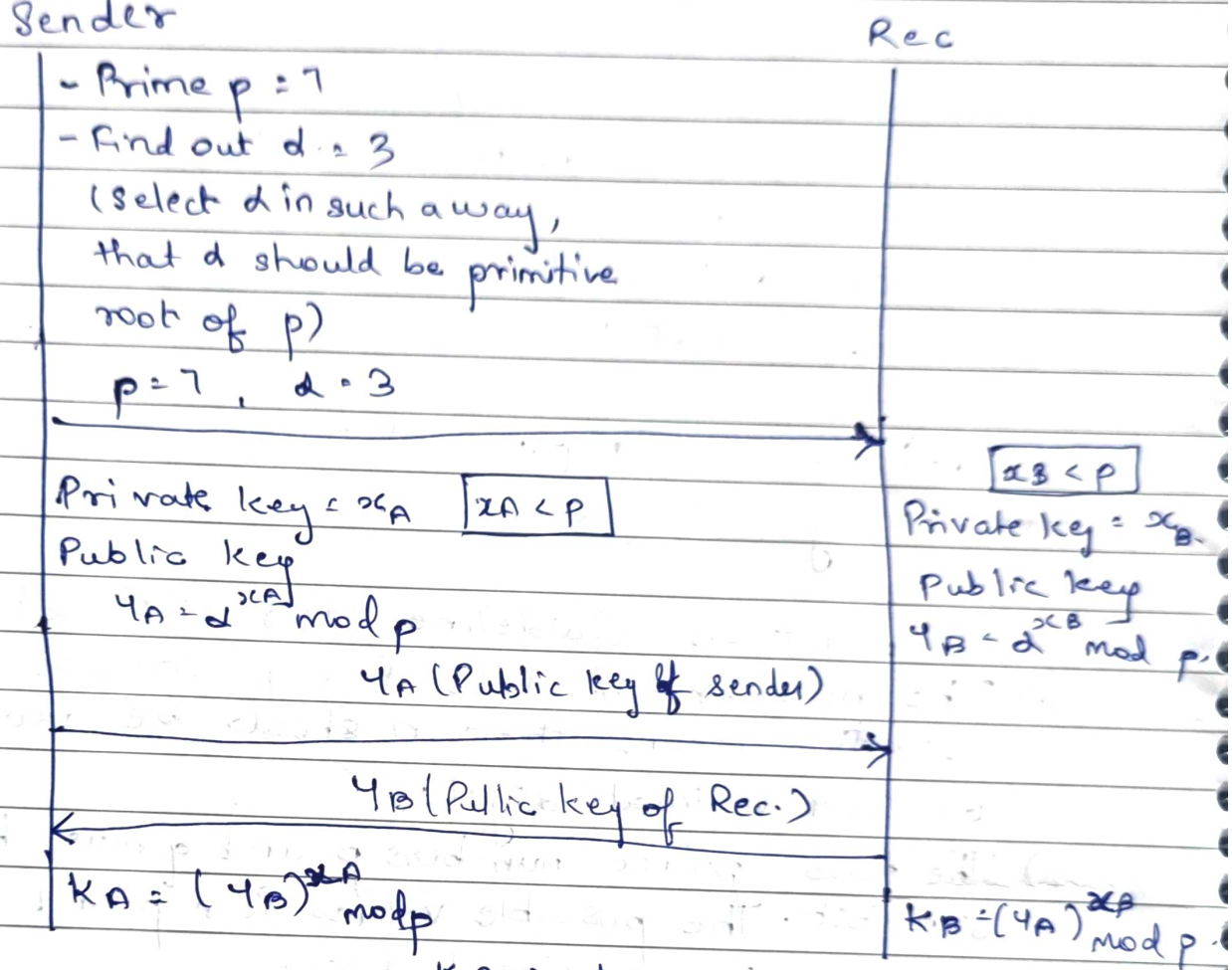
2.) The two prime numbers p and q must be atleast 512 bit. The possible values for p and q are 2^{512} or 154 decimal digit.

3.) User needs to select larger modulus value.

4.) Modulus value should not be shared with anyone or anybody. Both (p-1), (q-1) should have atleast one large prime factor.

5.) If private key (d, n) is compromised user or sender should change it immediately.

* Diffie-Hellman Algo:
- Key Exchange Algo:



p = 7 primitive Root of p (α)
(2, 3, 4)

$2^1 \bmod 7 = 2$
$2^2 \bmod 7 = 4$
$2^3 \bmod 7 = 1$
$2^4 \bmod 7 = 2$

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 2$
$3^3 \bmod 7 = 6$
$3^4 \bmod 7 = 4$
$3^5 \bmod 7 = 5$
$3^6 \bmod 7 = 1$

p = 7 (1 ..... 6)

__/__/____

EX: If $p = 7$ then; i) Find out primitive root of p.
ii) Find out public key of Alice.
iii) Find out public key of Bob.
iv) Find out Symmetric key of Alice as well as Bob.

Soln: i) $p = 7$, $\alpha = 3$. ii) private key $= 4 = x_A$.
Public key of Alice
$y_A = 3^4 \bmod 7$
$y_A = 4$

iii) private key $= 2 = x_B$.
Public key of Bob
$y_B = 3^2 \bmod 7$
$y_B = 2$

iv) $k_A = (2)^4 \bmod 7$ $\qquad k_B = (4)^2 \bmod 7$
$= 16 \bmod 7$ $\qquad = 16 \bmod 7$
$= 2$ $\qquad = 2$

$\therefore k_A = = k_B$

- Man in middle Attack: